Exclusif : 47 grandes entreprises françaises ciblées par une tentative d’escroquerie à grande échelle | Le Net Expert Informatique

	47 grandes entreprises françaises ciblées par une tentative d’escroquerie à grande échelle

Selon nos informations, une cinquantaine de grandes entreprises sont actuellement – ou ont été au cours des derniers jours – la cible d'un réseau criminel spécialisé dans l'escroquerie aux faux ordres de virement (FOVI), encore appelée « Arnaque au président ». La technique n'est pas nouvelle. Ce qui interpelle, dans le cas présent, c'est l'ampleur de l'offensive mise à jour.

« L'arnaque au président » n'est pas vraiment d'un genre nouveau. D'ailleurs son pionnier, Gilbert Chikli, poursuivi par 33 banques et aujourd'hui réfugié en Israël, vient d'être condamné par contumace à 7 ans de prison et à 1 millions d'euros d'amende.

En cause : des escroqueries jugées « hors-norme », dont l'essaimage est devenu en quelques mois la bête noire des grandes directions financières, à commencer par celles que l'on pensait être les plus aguerries. Ainsi en 2012, c'est KPMG qui en a fait les frais : le géant mondial de l'audit et du conseil en fiscalité a laissé s'envoler à son insu pas moins de 7,6 millions d'euros.

Ces tentatives d'escroquerie n'épargnent personne : pas plus Michelin ou le Palais de l'Elysée, que nos PME régionales. Si Gilbert Chikli promet aujourd'hui avoir tiré sa révérence, il n'est en revanche pas improbable qu'il ait, directement ou non, inspiré quelques disciples.

47 entreprises sous la menace imminente de la criminalité financière

C'est une longue liste de cibles que s'est procuré la rédaction du JDE, par l'intermédiaire d'un cabinet privé spécialisé dans l'investigation et la lutte anti-fraude. Pour des raisons évidentes de sécurité, les consultants qui nous ont transmis cette information préfèrent rester anonymes.

Ils témoignent : « la spécificité de cette affaire réside dans l'ampleur de l'attaque. A ce jour, nous ne pouvons confirmer son état de progression ou son éventuel aboutissement. Nous avons contacté chacune des entreprises ciblées pour tenter d'être mis en relation avec les directions générales ou financières afin de de les en avertir. Malheureusement, le personnel n'étant pas toujours sensibilisé à ce type de risque, certains de nos appels sont restés sans suite. »

Une situation qui n'étonne guère ces analystes rompus à la gestion des affaires réservées des dirigeants : «Malheureusement, ces escroqueries aboutissent la plupart du temps à cause de défaillances dans la sûreté et les procédures internes de l'entreprise. La formation des collaborateurs, la circulation intelligente de l'information et l'instauration de procédures de vérification restent les meilleurs remparts contre ces attaques. »

Parmi les entreprises ciblées ou déjà attaquées, recensées par les enquêteurs, on retrouve de grands noms de l'économie française, des groupes familiaux plus discrets, et des enseignes bien connues des Français. « Des attaques qui sont en préparation depuis fin avril », précisent nos interlocuteurs, qui nous livrent ci-après le nom des entreprises ou organismes concernés :

Direction Finance, Ludendo, Système U, Abbott, 3 Suisses, GE Capital, Sonepar, Joué Club, Monoprix, BHR Béton, La Redoute, Eurofactor, Sephora, Picard, Imerys, Groupe Flo, GSF, DB Apparel, Optic 2000, Marionnaud, Groupe Pigeon, Invacare, Franck Provost, Auchan, Continental Corporation, Pronatura, Finifac, Provalliance, Carrefour, Vivendi, Korian, Accor, Servair, Bricorama, SKF, SNEF, SNCF, Rexel, Ecolab, Soprasteria, Chausson Matériaux, Faurecia, Immochan, Eiffage, Clemessy.

Comment réagir en cas d'attaque ?

« Nous avons pris des mesures directes pour tenter d'endiguer la marge de manœuvre des 'assaillants' et prévenir le risque d'escroquerie, et travaillons en étroite relation avec nos partenaires depuis plus d'un mois, expliquent les analystes. Surtout, nous accompagnons nos clients dans la mise en place d'une procédure judiciaire à l'encontre des auteurs de la tentative d'escroquerie, en sachant pertinemment qu'elle sera longue et complexe. »

D'après le cabinet, en effet, les quelques traces électroniques analysées laissent apparaître un mode opératoire assez classique, probablement piloté depuis Israël ou un territoire voisin comme l'indiquent les paquets de données qui ont été analysés.

« Dans certains pays, les moyens de paiement prépayés sont très répandus et peu régulés, donc difficilement traçables. Ils peuvent être ensuite utilisés en France, pour acquérir de l'information légale sur les sociétés ou à l'étranger, pour recourir anonymement aux services d'une plateforme téléphonique ». Ce sont également ces cartes prépayées qui, en toute vraisemblance, auront permis aux escrocs de réserver des noms de domaine pour peaufiner leur déguisement électronique.

Un déguisement qui va, selon les experts, jusqu'à l'usurpation d'identité de personnes vivantes ou décédées : « Pour brouiller les pistes, ces brigands 2.0 utilisent vos adresses, numéros de téléphone, dates de naissance pour réserver des noms de domaine et procéder à certaines formalités en ligne. C'est probablement supposé divertir les enquêteurs », ironise l'un de nos experts.

Piqûre de rappel : le mode opératoire

Une opération couronnée de succès est une opération bien préparée. Les escrocs commencent par une phase de renseignement en « zone grise », en collectant un maximum d'informations sur leur cible. C'est ce qu'on appelle le « social engineering », dont le but est de recueillir suffisamment de données quant à l'environnement humain (personnes clés, numéros de téléphone, adresse email) et économique (contrats, fournisseurs, bilans, etc.) de l'entreprise.

C'est bien moins compliqué qu'il n'y paraît : munis d'une carte prépayée, il leur suffit de se rendre sur une base de données de type Infogreffe et de télécharger les documents les plus riches en information : derniers statuts et actes déposés, PV d'assemblées générales, ou comptes annuels par exemple. L'identification, sur les réseaux sociaux, des « personnes clés » dans l'organigramme de la cible permet parfois de se familiariser avec leurs futurs interlocuteurs.

Depuis une plateforme téléphonique située à l'étranger, mais avec un numéro français d'apparence, l'escroc appelle un directeur financier, un service comptable, ou tout individu ayant compétence à agir sur les comptes de l'entreprise.

Se faisant généralement passer pour le dirigeant de l'entreprise, il déploie alors des trésors de créativité et/ou de séduction. Tantôt flatteur, tantôt menaçant, il prétexte une situation d'urgence (opération boursière sensible, ou imminence d'un contrôle fiscal par exemple) et exige le virement immédiat d'une importante somme sur un compte habituellement hébergé en Chine.

Nos interlocuteurs invitent donc les entreprises à la plus grande vigilance : « ces offensives sont généralement fulgurantes et, le temps de réagir, nos escrocs sont déjà loin »…

Source : http://www.journaldeleconomie.fr/Exclusif-47-grandes-entreprises-francaises-ciblees-par-une-tentative-d-escroquerie-a-grande-echelle_a2456.html

L’anonymat du WHOIS remis en question à l’ICANN | Le Net Expert Informatique

	L’anonymat du WHOIS remis en question à l’ICANN

Une proposition de l'ICANN s'est attiré les foudres des commentateurs et de l'EFF. La suggestion propose de rendre impossible l'anonymisation des données personnelles sur le service WHOIS pour les sites à vocation commerciale.

Le service WHOIS est un outil particulièrement utile pour savoir qui se cache derrière un nom de domaine et comment contacter les responsables d'un site. Fourni par les registres de noms de domaines, il permet d'interroger les bases de données des bureaux d'enregistrement afin de connaître le nom et l'identité de la personne ou de la société détenant le nom de domaine, ainsi que certaines informations de contacts.
Ces informations ne sont pas forcement accessibles à tout le monde : dans de nombreux cas et pour éviter de voir ces informations personnelles à l'air libre, les bureaux d'enregistrement proposent un service d'enregistrement via proxy permettant de dissimuler au public les données et de les réserver aux seules personnes munies d'autorisations légales fournies par un service judiciaire national. Le service agit donc comme un écran afin d'offrir un moyen de contacter le propriétaire du nom de domaine tout en protégeant ses données personnelles.
Mais une proposition de l'ICANN, ouverte depuis mardi aux commentaires publics, envisage de revenir sur le fonctionnement de ce système en ouvrant à tous les données WHOIS des sites à but commercial. Selon l'EFF, cette règle s'appliquant « à tous les sites commerciaux » pourrait toucher de nombreux petits administrateurs de sites et de communautés en ligne qui ont choisi de mettre en place de la publicité ou un système de dons pour subvenir au coût de leur site.
L'EFF cite ainsi l'exemple de TG Storytime, un paisible site de fanfiction à destination des communautés LGBT, qui pourrait ainsi se voir obligé de révéler certaines informations personnelles liées à l'administrateur du site si la nouvelle proposition était approuvée par l'ICANN.

L'EFF dans la boucle
L'EFF explique que ce changement est notamment soutenu par le secteur du divertissement, qui entend ainsi simplifier les procédures judiciaires à l'égard des sites diffusant des contenus constituant des infractions relatives à la propriété intellectuelle. Outre le risque que cette proposition peut faire peser sur les données personnelles des utilisateurs, on peut également évoquer les dangers relatifs à la cybersécurité.
Cedric Pernet, dans son ouvrage sur les Advanced Persistent Threat, citait ainsi les informations de service WHOIS parmi la liste des sources utiles aux attaquants pour préparer leurs attaques, en leur permettant d'identifier précisément le bureau d'enregistrement d'un site, un numéro de téléphone ou encore le nom de l'employé chargé d'administrer le nom de domaine.Autant d'informations utiles pour une attaque de type spear phishing.
La proposition est ouverte aux commentaires jusqu'au 7 juillet, et suscite déjà un certain engouement de la part des opposants à ce changement de politique, qui ont déjà posté des milliers de commentaires invitant l'ICANN à refuser cette proposition.

Source : http://www.zdnet.fr/actualites/l-anonymat-du-whois-remis-en-question-a-l-icann-39821566.htm
Par Louis Adam

Un centre de compétence Kaspersky doit être mis en place très prochainement au Gabon | Le Net Expert Informatique

Un centre de compétence Kaspersky doit être mis en place très prochainement au Gabon

Un centre de compétence Kaspersky doit être mis en place très prochainement au Gabon, selon les termes d'un accord de partenariat signé mardi à Libreville entre l'Agence nationale des infrastructures numériques et des fréquences (Aninf) et l'éditeur Kaspersky.

En vertu de cet accord, signé par le directeur général de l'Aninf, Alex Bernard Bongo Ondimba et le vice-président de Kaspersky, Veniamin Levtsov, le futur centre, qui aura, par ailleurs, une vocation sous régionale, doit permettre au Gabon d'assurer la veille, la détection, l'analyse et la prévention des cyber-attaque.

« Ce partenariat est très salutaire pour le Gabon du fait qu'il nous permettra de nous doter d'un véritable système de défense en matière de virus et en ce qui concerne la cybercriminalité », a déclaré M. Alex Bernard Bongo Ondimba.

Outre la mise en place d'un centre de compétence au Gabon, l'accord signé porte également sur le transfert des compétences dans les domaines de la sécurité industrielle et de la cybercriminalité.

'Nous entendons contribuer à sauver le monde en mettant en place des systèmes de lutte contre des attaques axées sur la cybercriminalité. Nous voulons également apporter nos compétences aux structures locales », a affirmé, pour sa part, M. Levtsov.

Implantée dans plusieurs pays d'Afrique et dans d'autres continents, Kasperky est une entreprise russe leader mondiale en matière de sécurité informatique.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
https://mail.google.com/mail/u/0/?hl=fr&shva=1#inbox/14e3b659f932c0fd?compose=14e2eb99aeedd11a

Grosse menace sur les mots de passe contenus dans le trousseau d’Apple | Le Net Expert Informatique

	Grosse menace sur les mots de passe contenus dans le trousseau d’Apple

Peu importe que vous utilisiez iOS ou OS X, vos mots de passe sont en danger s'ils sont stockés dans le trousseau d'Apple.

Des chercheurs universitaires ont découvert une énorme faille de sécurité chez Apple, une faille suffisamment importante pour que la marque à la pomme n'ait pas encore réussi à la corrigé alors qu'elle a été signalée au mois d'octobre dernier. Pour causse, elle touche le mécanisme censé protéger les mots de passe : le trousseau.
L'idée du trousseau est simple : centraliser les identifiants et mots de passe pour que l'utilisateur n'ait pas à les ressaisir. Le problème, c'est que des chercheurs universitaires ont découvert toute une série de failles de sécurité.
Alors que le bac à sable est censé isoler les données pour qu'elles soient protégées, les chercheurs sont parvenus à percer le mécanisme.
Ils ont aussi créé un malware capable d'afficher tous les mots de passe de l'Apple's Keychain, c'est-à-dire ceux stocker dans le trousseau, ce qui expose tous les identifiants utilisés par les applications tierces : Facebook, Twitter, iCloud, Gmail, etc.
« Nous sommes parvenus à pirater tout le service Keychain, où Apple stocke les mots de passe et les autres paramètres de ses applis ainsi que les sandbox containers' dans OS X », explique Luyi Xing, responsable de cette recherche. « Nous avons découvert de nouvelles faiblesses dans les mécanismes de communication entre applis au sein d'OS X et d'iOS, qui pourraient être exploitées pour dérober des données confidentielles d'Evernote, Facebook et d'autres applis largement utilisées. »
Pour l'heure, le problème est énoncé, mais aucune solution n'est pour le moment encore disponible, le problème subsiste dans les versions actuelles d'iOS et d'OS X.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.linformatique.org/grosse-menace-sur-les-mots-de-passe-contenus-dans-le-trousseau-dapple/

Les nouvelles cibles de la

Cybercriminalité | Le Net Expert Informatique

Les nouvelles cibles de la Cybercriminalité

Le piratage de TV5 Monde il y a quelques semaines est symptomatique du futur qui se prépare en matière de cybercriminalité. A mesure que les attaques deviennent plus sophistiquées, les pirates se rapprochent des infrastructures critiques. Ainsi, l'an passé, 43 % des entreprises œuvrant dans l'énergie (mines, compagnies du gaz, pétrolière) ont été la cible des cybercriminels au moins une fois dans l'année, rapporte une étude Symantec. Même constat chez Trend Micro, qui pointe que 47 % de l'industrie a fait l'objet d'une attaque, soit plus que les sites gouvernementaux. « Les attaques contre les infrastructures critiques deviennent une préoccupation grandissante de tous les gouvernements. En raison des conséquences potentielles des attaques, ces sites sont devenus très attractifs pour les pirates », dit l'étude de Trend Micro.

13,2 millions d'euros par an

Les dommages commis par les cybercriminels coûtent 13,2 millions d'euros par an à chaque entreprise de l'énergie, soit plus que dans n'importe quelle industrie, selon une étude réalisée par Poneman pour HP, relayée par Bloomberg. Pour se protéger, le secteur énergétique devrait porter son investissement en cybersécurité à 1,9 milliard de dollars d'ici à 2018, note ABI Research. Depuis quelques années, les exemples d'attaques contre des sites sensibles se multiplient. En France, le spécialiste du nucléaire Areva a avoué en 2011 que des pirates s'étaient introduits dans son réseau informatique pendant deux ans. En 2012, la compagnie pétrolière Aramco a vu 30.000 de ses ordinateurs infectés par un virus. Après avoir subi l'assaut des Anonymous, sorte de Robin des bois autoproclamés du Net, la compagnie nationale du pétrole koweïtien a déconnecté ses trois raffineries d'Internet. Sans être certaines d'être immunisées contre le fléau. Stuxnet, le virus conçu pour attaquer les sites nucléaires iraniens, s'est propagé sur des sites qui n'étaient pas connectés à Internet.

Afin de garder un temps d'avance sur des grands groupes qui se protègent mieux qu'hier, les cybercriminels font évoluer leurs méthodes. Pour atteindre leur cible, ils passent de plus en plus par des sous-traitants ou des fournisseurs. Pour preuve, les entreprises de B to B (commerce interentreprise) ont été ciblées par 15 % des 6 milliards d'attaques répertoriées en 2014 par NTT Com Security.

En attendant, si la crainte d'un virus qui ferait dérailler un train ou plongerait une ville dans le noir est dans tous les esprits, l'essentiel de la cybercriminalité a encore des motifs financiers. L'an passé, 18 % des attaques ont visé des institutions financières, devançant tous les secteurs d'activité.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.lesechos.fr/tech-medias/hightech/021137768977-cybercriminalite-les-nouvelles-cibles-1128488.php
Par Sandrine Cassini

Un réseau de fraude de clés de connexion Internet démantelé | Le Net Expert Informatique

	Un réseau de fraude de clés de connexion Internet démantelé

La brigade ville de la gendarmerie de Bogodogo vient de mettre hors d'état de nuire un réseau qui disposerait de clés de connexion internet de l'ONATEL SA à navigation illimitée.

La cybercriminalité est en pleine expansion au Burkina Faso. Face à ce fléau, le commandement de la Gendarmerie a décidé de lancer une opération d'envergure.
C'est ainsi que la Brigade ville de Bogodogo découvre par une source digne de foi, un réseau de vendeurs de clés de connexion de l'ONATEL SA sur le marché noir, selon le Colonel Sam Djiguiba Ouédraogo, Commandant du groupement départemental de la Gendarmerie de Ouagadougou.
Une enquête ouverte à cet effet a permis de mettre la main sur un auteur principal et trois complices.

La gendarmerie invite la population à la vigilance
Technicien d'exploitation et de maintenance à l'ONATEL SA, l'auteur de la fraude profite de son accès à la base technique pour activer des clés de connexions internet déjà résiliées ou suspendues pour en faire des clés de connexion à navigation illimitée.
Il les met ensuite sur le marché noir par l'intermédiaire de ses complices à des prix variant de 50 000 F CFA à 250 000 F CFA, soutient le commandant de la gendarmerie.
Une fois de plus, la gendarmerie invite la population à la vigilance et à signaler aux forces de sécurité toutes activités suspectes.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://burkina24.com/2015/06/24/cybercriminalite-un-reseau-de-fraude-de-cles-de-connexion-internet-demantele/
Par Serge Balma (stagiaire)

Un hacker cloue plusieurs avions au sol | Le Net Expert Informatique

Un hacker cloue plusieurs avions au sol

Une attaque informatique subie par la compagnie polonaise LOT a causé l'annulation de 20 vols dimanche.

Des hackers qui clouent des avions au sol. Ce n'est pas le scénario d'un film catastrophe, mais la mésaventure subie dimanche par la compagnie polonaise LOT et racontée par CNN.
Les ordinateurs au sol piratés. Tout a commencé à l'aéroport Chopin de Varsovie, où la compagnie dit avoir été victime d'une attaque. Ses ordinateurs au sol, utilisés pour créer les plans de vols, ont subi une attaque. Résultat : impossible de créer des plans de vols pour les avions au départ de la capitale polonaise.
Au total, la compagnie polonaise a dû annuler pas moins de 20 vols et plusieurs autres ont subi des retards. Quelque 1.400 passagers ont ont été affectés. Une enquête a été ouverte, mais les autorités ignorent l'identité des hackers.
Un hacker arrêté en mai. Ce n'est pas la première fois que des hackers illustrent la vulnérabilité des compagnies aériennes : fin mai, un pirate américain a été arrêté par le FBI après s'être vanté sur Twitter d'avoir réussi à hacker un avion en plein vol. Il assure s'être connecté au système informatique de l'avion et avoir légèrement modifié la trajectoire de l'avion, afin de démontrer les faiblesses du système de sécurité aérien.

Source : http://www.europe1.fr/international/un-hacker-cloue-plusieurs-avions-au-sol-1359726

Une convention internationale pour lutter contre le cybercrime | Le Net Expert Informatique

	Une convention internationale pour lutter contre le cybercrime

En avril 2015, la société Symantec spécialisée dans la sécurité informatique présentait son rapport annuel. Selon ses dires, en 2014, 317 millions de nouveaux programmes malveillants auraient été crées au niveau mondial. Enfin, faut-il rappeler ce qui est arrivé à nos amis de TV5 Monde, il y a de cela quelques semaines ? Ecran noir pour la chaîne les 8 et 9 avril 2015. Sans que pour le moment on sache d'où vient l'attaque.

C'est une évidence, la cybercriminalité est en pleine croissance. Multiforme, mondialisée, l'œuvre d'un petit génie malfaisant, ou d'organisations criminelles quand il ne s'agit pas d'une nouvelle arme d'Etat. Une pieuvre, Octopus…

La Convention de Budapest

Pour le moment, le seul grand texte international existant dans le cadre de la lutte contre ce type de criminalité est l'œuvre du Conseil de l'Europe. Signée à Budapest en novembre 2001, la convention traite des infractions possibles à l'égard des droits d'auteur, de la sécurité des réseaux informatique, des fraudes en général et aussi à la lutte contre la pornographie enfantine. Un texte unique en son genre, qui dépasse le seul cadre du Conseil de l'Europe. Puisque déjà 66 pays du monde entier ont adhéré. Dernier en date, il y a de cela quelques jours le Sri Lanka.

Que ce soit le Conseil de l'Europe qui est en pointe dans ce combat ne paraît pas illogique. Comme le rappelle le spécialiste de cette lutte au sein du Conseil de l'Europe, Alexander Seger, ce sont les droits de l'Homme et la démocratie qui sont en danger.

Ce texte permet avant tout de mener la bataille du droit. Il n'a pas de rapport avec les lois en cours sur le renseignement et qui font beaucoup la Une dans de nombreux pays dont la France. En revanche, devant la croissance de ce type de criminalité et le développement toujours plus rapide de la technique, ce texte doit constamment évoluer de même que les pratiques des autorités. Ainsi le Conseil de l'Europe vient-il de créer à Bucarest un bureau destiné à encadrer et à proposer une aide technique aux juristes ou aux politiques lancés dans ce combat.

De même, tous les 18 mois, une grande réunion internationale se tient avec tous les acteurs concernés. C'est cette réunion qui répond au doux nom d'Octopus. La dernière se tient à Strasbourg ces jours-ci. Ces conférences permettent de faire le point sur de nouvelles pratiques problématiques qui apparaissent. Ainsi sur le droit des victimes passablement oubliées pour le moment ou bien encore, et ce sera le thème principal des travaux, sur la difficulté pour la justice de trouver des preuves informatiques. Dans quel disque dur les trouver, quel nuage explorer ? En rappelant à nouveau qu'il ne s'agit là que d'un texte portant sur le judiciaire.

Il y a quelques semaines, à La Haye, s'est tenu également une Conférence mondiale sur le Cyber espace 2015. Cette rencontre qui prend en compte les extraordinaires possibilités qu'offre internet avait pris en compte également la question de la sécurité qui doit régner dans le cyberespace. La prise de conscience est donc bien là, il faut espérer que les techniques des criminels quels qu'ils soient n'aillent pas en se développant plus vite que les solutions. Or, et l'on revient à l'étude annuelle de Symantec, il faut désormais aux éditeurs de logiciels beaucoup plus de temps pour créer et déployer des correctifs en cas de faille sécuritaire.

Et s'il fallait vous convaincre du problème, un dernier exemple, celui des « rançongiciels ». Ils prennent le contrôle de vos PC et vous piquent littéralement vos données rendues plus tard contre rançon. Une entreprise française s'est vu réclamer ainsi 90.000 euros.

Et vous, si vous êtes amateurs de pizzas, vous risquez gros…

Lire la suite….

Source : http://geopolis.francetvinfo.fr/une-convention-internationale-pour-lutter-contre-le-cybercrime-65027

La contradiction est manifeste entre la perception des salariés et la réalité en matière de cybersécurité | Le Net Expert Informatique

←	La contradiction est manifeste entre la perception des salariés et la réalité en matière de cybersécurité

Les salariés français ont une connaissance relativement précise des notions liées à la cybersécurité des entreprises. Même si les cyberattaques semblent relativement fréquentes, ils jugent leur entreprise relativement bien protégée sur ces enjeux même si tous ne connaissent pas en détail sa politique en matière de sécurité. Dans ce cadre, ils identifient comme principales menaces : les virus informatiques, le vol de données et la perte de données liée à une erreur humaine. Tels sont les principaux constats que l'on peut tirer de la première étude* portant sur la cybersécurité vue par les collaborateurs, dévoilée ce 17 juin au Bourget par Capgemini et Sogeti.

Selon l'étude « Cybersécurité, Objets connectés et Systèmes industriels », les salariés français ont dans leur ensemble une connaissance assez précise des différentes notions liées à la cybersécurité : plus des trois quart estiment savoir précisément ce qu'est un virus informatique (88%), un hackeur (80%), un pare-feu (75%) ou une cyberattaque (75%). Seuls les salariés « seniors » sont plus hésitants, même si une majorité d'entre eux reste familier avec ces termes.
Dans ce cadre, 85% des salariés estiment que leur entreprise est bien protégée contre les attaques informatiques et les hackeurs. C'est plus particulièrement le cas des salariés des grandes entreprises pour lesquels ce score monte à 90% (contre 75% pour les PME). Ils jugent ainsi dans leur grande majorité la politique de sécurité informatique de leur entreprise adaptée à leur secteur (85%), efficace (85%) et claire (72%). Elle mériterait toutefois d'être davantage connue (61%).
36% des salariés déclarent que leur entreprise a déjà fait l'objet d'une cyberattaque. Ce score monte à 47% pour les salariés des grandes entreprise. Or, selon Kaspersky, plus de 90% des entreprises ont déjà subi une attaque informatique. Plus spécifiquement, 19% des salariés ont connu une attaque informatique de leur ordinateur professionnel. Pour 5% cela est même régulier. On remarquera que les salariés des PME sont plus nombreux a avoir subi ce type d'attaque que ceux des grandes entreprises. En revanche seule une minorité s'est déjà fait voler du matériel informatique professionnel : 8% un ordinateur, 6% leur téléphone portable. « Ces chiffres contradictoires montrent la complexité de la cybersécurité : celle-ci représente un risque asymétrique pour l'entreprise. Tous les chiffres indiquent que le nombre d'attaques croît considérablement d'année en année (120% de 2013 à 2014) ; attaques dont les salariés de l'entreprise n'ont pas nécessairement connaissance », commente Bernard Barbier, Responsable de la Sécurité des Systèmes d'Information du groupe Capgemini.
Cette contradiction entre la perception des salariés et la réalité de la menace est également illustrée dans le sondage par un fort sentiment de sécurité parmi les salariés. 65% d'entre eux estiment en effet que leur entreprise est plutôt bien protégée, et 20% très bien protégée contre les attaques informatiques et les hackeurs. Ce sentiment est surtout partagé au sein des ETI4 (93%) et des grandes entreprises (90%). « Ce sentiment de sécurité des salariés (65%) est une fois encore en totale contradiction avec les résultats de récentes études démontrant que les campagnes de phishing sont d'une très grande efficacité et qu'elles représentent plus de 80% des attaques réussies. En réalité, il suffit d'un seul PC infecté pour entraîner de lourdes conséquences financières et de réputation pour l'entreprise. On peut par ailleurs se demander si ce sentiment de sécurité n'entraîne pas un manque de vigilance des salariés dans le traitement des messages électroniques venant de l'extérieur de l'entreprise », explique Bernard Barbier.

Au final, les salariés ont trois grandes craintes quand à la cybersécurité de leur entreprise : les virus informatique (pour 48%), le vol de données (43%) et la perte de données suite à une erreur humaine (38%). On notera que les craintes sont fortement liées au secteur d'activité de l'entreprise. Ainsi les salariés de l'industrie craignent davantage le vol de données tandis que ceux du commerce ou du BTP pointent davantage les virus informatiques.

Le vol des données informatiques constitue le premier motif de crainte des salariés. Pour 23% d'entre eux, cela constitue même la plus grosse menace informatique qui pèse sur leur entreprise. De plus, 10% des salariés déclarent avoir subi un vol de leur ordinateur professionnel. « Ces chiffres démontrent la nécessité de protéger les données qui sont au cœur de l'activité de l'entreprise. La priorité est par conséquent de mettre en place des politiques de chiffrement des données : chiffrement des emails et des PC portables », poursuit Bernard Barbier.

Et de préciser que « ce sondage souligne que les salariés de l'entreprise ont un sentiment positif quant à la sécurité de leur système d'information classique. En revanche, la perception du niveau de sécurité des systèmes industriels (contrôle commande des usines) semble avoir plusieurs années de retard car la cyber menace est plus récente. Pourtant, le danger est plus dramatique encore, avec des conséquences matérielles et humaines, comme dans l'hypothèse d'une explosion d'usine. Le cyber terrorisme pourrait d'ailleurs viser en priorité ce domaine dans un avenir proche ».

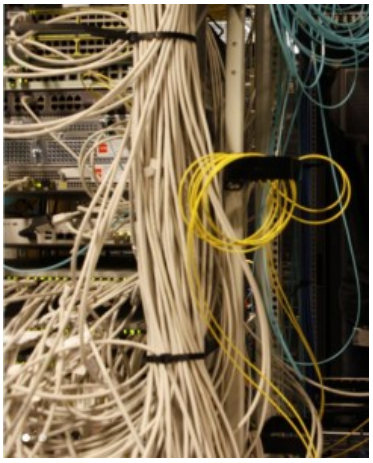
Didier Appell, responsable, au sein de l'entité sectorielle mondiale « Cybersecurité » du Groupe, de l'offre Cybersécurité industrielle de Sogeti High Tech, le pôle d'expertise en Ingénierie et conseil en technologies du groupe Capgemini, précise : « Les entreprises ont fourni de gros efforts pour sensibiliser leurs salariés aux risques que représentent les attaques cybernétiques. Par extension, cette sensibilisation doit être également portée sur les systèmes industriels de supervision, de commande et contrôle ainsi que des systèmes embarqués car là aussi nous relevons une contradiction entre la perception des salariés et la réalité des menaces. Nous sommes effectivement de plus en plus sollicités par nos clients pour les aider à renforcer leur sécurité sur tous ces aspects ».

* L'étude a été réalisée auprès d'un échantillon de 1010 salariés français de bureau d'entreprises privées. La représentativité de l'échantillon est assurée selon la méthode des quotas sur les critères de sexe, d'âge, de catégorie socioprofessionnelle, de taille d'entreprise, de secteur d'activité de l'entreprise, de statut de l'employeur (public/privé) et de région de résidence. L'échantillon a été interrogé en ligne sur système CAWI (Computer Assistance for Web Interview) du 13 au 26 mai 2015.

Source : http://www.infodsi.com/articles/156643/contradiction-est-manifeste-entre-perception-salaries-realite-matiere-cybersecurite.html

---

Le business des écoutes et des données personnelles | POLICEtcetera | Le Net Expert Informatique



Le business des écoutes et des données personnelles

Au moment où les États-Unis sont en train – timidement – de faire machine arrière sur le Patriot Act, la France se dote d'une véritable armada de machines électroniques pour surveiller ses propres ressortissants – et à l'occasion, les étrangers de passage dans notre beau pays. Dans cette guerre secrète contre le crime et le terrorisme, qui s'est amplifiée ces dernières années, pas de chars, pas d'avions, pas d'armes, mais un chiffre d'affaires en pleine érection. On peut se demander à qui profite le crime et combien cela va nous coûter… Dans quelle poche va-t-on prendre les sous ? Au détriment de quels services publics ?…

Nous sommes tellement habitués à ces projets qui capotent, comme Ecomouv ; ou d'autres qui aboutissent, mais dont la facture a été multipliée par 2, 3, 4…
Tiens, par exemple, parlons de la plateforme nationale d'interceptions judiciaires (PNIJ). En 2007, il était question d'une enveloppe de 17 millions d'euros. En 2010, elle était de 42 millions, et en 2014, de 47. En cette année 2015, alors que les premiers essais ont commencé dans certains services de police et de gendarmerie sur le ressort des cours d'appel de Paris, Versailles et Rouen, on se rapprocherait des 55 millions. C'est du moins ce que dit Le Canard enchaîné daté du 20 mai 2015, ajoutant malicieusement, que, pour l'instant, seuls les clients d'Orange peuvent être mis sous écoute.
En fait, l'addition sera beaucoup plus lourde, car, parallèlement, les fournisseurs d'accès à Internet ont dû effectuer des travaux et notamment déployer des fibres optiques jusqu'à Élancourt, dans les Yvelines, sur le site de Thales qui accueille la PNIJ. Il faut également revoir les réseaux des services de police, de gendarmerie, des douanes… Lors du jeu de questions à l'Assemblée Nationale, le député Alain Tourret a avancé un surplus de 50 millions. Il n'a obtenu ni confirmation ni infirmation de ce chiffre, la garde des Sceaux se contentant de dire qu'il était prévu que le ministère de l'Intérieur participe au pot commun.
Et l'addition n'est pas close, car il pourrait se révéler nécessaire de renforcer la sécurité de la PNIJ. On se souvient des propos tenus lors du débat sur la loi sur le renseignement : la centralisation des données dans un même lieu géographique « pourrait constituer une source de vulnérabilité importante ». La centralisation nationale des réquisitions judiciaires constitue donc une faiblesse dans la sécurité, ce que policiers et magistrats n'ont cessé de clamer depuis que l'idée est dans l'air. D'autant que cette plateforme, contrairement à ce que son nom peut laisser penser, n'est pas seulement destinée à intercepter les communications téléphoniques : c'est un système complet de traitement automatisé de données à caractère personnel. Une machine qui va brasser et enregistrer les données personnelles de toutes les personnes impliquées ou suspectées dans une affaire judiciaire.
Une caverne d'Ali Baba sur laquelle les services de renseignement, français ou étrangers, vont forcément loucher. À ce sujet, on peut d'ailleurs s'interroger sur la portée exacte de l'amendement de dernière minute (un de plus) présenté par le gouvernement à la loi sur le renseignement : les services habilités pourront avoir accès aux traitements automatisés de données à caractère personnel, y compris celles des procédures judiciaires en cours. Il s'agit pour ces services, nous dit-on, de pouvoir consulter le TAJ, c'est-à-dire le fichier d'antécédents judiciaires (qui a remplacé le STIC de la police et le JUDEX de la gendarmerie). Mais alors, pourquoi ce pluriel dans l'article L.234 : « pourront avoir accès aux traitements automatisés… » Cela vise-t-il également le fichier Cassiopée du ministère de la Justice et la PNIJ ?
Je vais finir parano !
Lire la suite….

Source : http://moreas.blog.lemonde.fr/2015/06/21/le-business-des-ecoutes-et-des-donnees-personnelles
par G.Moréas